



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,715	12/12/2000	David Michael Kurn	20206-034(P00-3416)	8318

7590

05/03/2004

Bill Streeter
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 05/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/736,715

Applicant(s)

KURN ET AL.

Examiner

Michael R Vaughan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☒ Claim(s) 12 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>2</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-13 have been examined and are pending.

Specification

Applicant is required to update the status (pending, allowed, etc.) of all parent priority applications in the first line of the specification. The status of all citations of US filed applications in the specification should also be updated where appropriate.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper No. 2, is attached to the instant Office action.

Drawings

Formal drawings received 4-30-01 are accepted.

Claim Objections

Claim 12 is objected to because of the following informalities: typo "Repository", --repository--. Appropriate correction is required.

Claim Rejections - 35 USC ' 101 Utility

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-12 are rejected under 35 U.S.C. 101 because the language of the claim 1 raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 USC 101.

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blakley et al, hereinafter Blakley (USP 6,067,623) in view of Microsoft Authenticode Technology, hereinafter MAT.

As per claims 1 and 13, Blakley teaches cryptographic system and method with at least one server and any number of clients, including none, the cryptographic system further comprising at least one application on one of the at least one server, each capable of engaging in a context-free multi-part communication session with any of the clients (column 4, lines 50-51);

a key repository process on one of the at least one server, the key repository process (column 5, lines 14-16) configured to validate and record authorizations of specific clients to access one or more than one set of symmetric keys, wherein each of the at least one application is configured to query the key repository process for one or more than one set of symmetric keys. Blakley teaches that the system of authentication can

be carried out through an SSL or SHTTP protocol (column 2, lines 9-11). SSL is a well-defined protocol. It is known in the art that once an SSL handshake has been completed a bulk cipher, including RC4 and DES, which both use symmetric keys, is used to encrypt the transferred data. Therefore, it is inherent from the teachings of Blakley that symmetric keys are utilized at the server for at least this purpose. One of ordinary skill in the art would assume they are also stored in the key repository. Also from the specifications of the SSL protocol, an authentication procedure must first be satisfied. Therefore the server would only provide the set of symmetric keys if the client has been authenticated. Blakley teaches the particular instance of the at least one application can utilize the one or more than one set of symmetric keys for securely off-loading sensitive information in any intermediate part of the context-free multi-part communication session (column 5, lines 25-30).

Blakley teaches every limitation of claim 1 either explicitly or implicitly with the exception of basing the authentication on a particular instance of one pre-authorized application. Blakley teaches that it is the client that is authorized. Blakley authorization method does not consider the application of the user to be authentic. Therefore an attacker who has stolen a login could use an altered version of a program to gain access to network resources. MAT teaches the use of Authenticode as a way of verifying that a program has not been tampered with (page 2). MAT teaches that end user and even corporations can benefit from this technology. Corporations can set up a list of pre-authorized programs that can be used to access the network (page 4). The Authenticode protects both the client and the server by providing a way to insure the

program has not been altered. Blakley's system would be more secure with this technology in place. Not only would the user be authenticated, the actual program that the user is using to connect with the server would be authenticated.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of MAT within the system of Blakley because it would add another level of security to protect the resources of the network. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 2, Blakley teaches the sensitive information in an intermediate part is securely off-loaded to a database (column 1, line 23).

As per claim 3, Blakley teaches this use of personal web browsers to log into a secure server. The clients initiate the HTTP protocol. The HTTP uses cookies to store login information so that a client does not have to keep reentering authorization information each time he/she tries to access a service of the network. Cookies are used to store this information on the client so that the user does not have to manually resend the information.

As per claim 4, Blakley teaches the key repository process maintains one set of symmetric keys for all of the at least one application (column 5, line 13).

As per claim 5, Blakley implicitly teaches symmetric keys. Examiner supplies the same rationale for the motivation to include the specific applications as recited in the rejection of claim 1. Because the keys are stored for each user (column 5, lines 13-15) it would have been obvious to also store the keys for each application. Certain applications only have the computing power to use keys of certain length. Also some applications would not need the strength of a long key than others. Therefore it would have been obvious to one of ordinary skill in the art to associate certain keys with particular applications because Blakely teaches associating keys with particular users and those users are using the applications to authenticate.

As per claim 6, Blakley teaches the text-free multi-part communication session is conducted using a hypertext transfer protocol (column 2, lines 15-20).

As per claim 7, Blakely teaches the at least one application and the at least one server utilize one of a hypertext markup language, a standard generalized markup language, and an extensible markup language (column 3, lines 60-65).

As per claim 8, Blakely teaches the securely off-loaded sensitive information can be then accessed by any one of the at least one application engaging in the 15 context-free multi-part communication session (column 5, lines 20-22).

As per claim 9, Blakley teaches the securely off-loaded sensitive information is encrypted (column 2, lines 5-10).

As per claim 10, Blakley teaches the sensitive data is securely off-loaded to a working memory in a server to enable a single server process instance to service all communications between the at least one application and the server (column 5, lines 18-22).

As per claim 11, Blakley teaches the use of web browsers which are typically used to spawn other instances such as applets or plug-ins (column 3, lines 60-61).

As per claim 12, Blakley teaches the key repository process is a process pair (column 5, line 50)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100